PCT/JP2004/008942

日本国特許庁
JAPAN PATENT OFFICE

26.07.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　６月２０日

出願番号
Application Number: 特願２００３－１７６５６９

[ST. 10/C]: [ＪＰ２００３－１７６５６９]

出願人
Applicant(s): 日本電信電話株式会社

２００４年　９月　２日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３０７８６７０

【書類名】　特許願
【整理番号】　NTTH155518
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/00
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　小野　久美子
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　立元　慎也
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　坂谷　精一
【特許出願人】
　【識別番号】　000004226
　【氏名又は名称】　日本電信電話株式会社
【代理人】
　【識別番号】　100077274
　【弁理士】
　【氏名又は名称】　磯村　雅俊
　【電話番号】　03-3348-5035
【選任した代理人】
　【識別番号】　100102587
　【弁理士】
　【氏名又は名称】　渡邉　昌幸
　【電話番号】　03-3348-5035

【手数料の表示】

【予納台帳番号】　013402

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9701395

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セッション制御サーバ、通信装置、通信システムおよび通信方法、ならびにそのプログラムと記録媒体

【特許請求の範囲】

【請求項１】　ネットワークを介してセッション制御サーバと通信可能に接続され、１以上の該セッション制御サーバを経由して他の通信装置との間で信号送受信により該他の通信装置とのセッションを確立する通信装置において、

送信信号の守秘性を保つために暗号化した信号を送信する際に、暗号化のための第一の暗号化鍵を生成する手段と、

該第一の暗号化鍵を用いて信号を暗号化する手段と、

該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段と、

暗号化された該第一の暗号化鍵を添付して、該第一の暗号化鍵で暗号化された信号を送信する手段とを備え、

該第一の暗号化鍵を第二の暗号化鍵で暗号化する手段は、信号内情報の開示のみもしくは開示と変更の両方を許容された１つのセッション制御サーバの第二の暗号化鍵により、第一の暗号化鍵を暗号化し、

該第一の暗号化鍵で暗号化された信号を送信する手段は、前記暗号化された第一の暗号化鍵と、該第一の暗号化鍵により暗号化された信号と、該セッション制御サーバに対する復号化要求指示、もしくは復号化要求指示と変更許容通知を送信することを特徴とする通信装置。

【請求項２】　ネットワークを介して複数の通信装置と他のセッション制御サーバと通信可能に接続され、発信側の通信装置もしくは該他のセッション制御サーバから送信された信号を受信し、受信された信号を着信側の通信装置もしくは該他のセッション制御サーバに送信することで、前記発信側の通信装置と前記着信側の通信装置とのセッションを確立させるセッション制御サーバにおいて、

暗号化した第一の暗号化鍵を添付して、該第一の暗号化鍵で暗号化された信号を受信する手段と、

自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗号化鍵を復号

化する手段と、

復号化して得た第一の暗号化鍵を用いて信号を復号化する手段と、

復号化して得た第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段と、

任意の第二の暗号化鍵で暗号化した後、復号化して得た第一の暗号化鍵を添付して、復号化して得た第一の暗号化鍵で暗号化されている信号を送信する手段とを備え、

前記受信手段が暗号化された信号を受信した際に、復号化要求の有無を判断し、該第二の暗号化鍵に対応した第二の復号化鍵で暗号化鍵を復号化するか、あるいは、該第二の暗号化鍵に対応した第二の復号化鍵で該暗号化鍵を復号化することで、復号化要求の有無を判断するか、あるいは、その両方を行うことにより、該第一の暗号化鍵を取得し、

前記信号復号化手段が該第一の暗号化鍵で暗号化された信号を復号化し、

さらに、前記暗号化手段は、信号送受信時に経由し、かつ開示のみあるいは開示と変更の両方を許容された前記他のセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、取得された第一の暗号化鍵を暗号化し、

前記送信手段は、該暗号化された第一の暗号化鍵と、取得された第一の暗号化鍵により暗号化されている信号と、第二の暗号化鍵が該他のセッション制御サーバの暗号化鍵である場合には、該他のセッション制御サーバに対する復号化要求指示、もしくは復号化要求指示と変更許容通知を送信すること

を特徴とするセッション制御サーバ。

【請求項３】　請求項２記載のセッション制御サーバにおいて、

前記各手段に加えて、送信信号の守秘性を保持するために暗号化した信号を送信する際に、暗号化のための新たな第一の暗号化鍵を生成する手段と、

生成した該第一の暗号化鍵を用いて信号を暗号化する手段と、

生成した該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段と、

該第二の暗号化鍵で暗号化した生成した第一の暗号化鍵を添付し、かつ該生成した第一の暗号化鍵で暗号化された信号を送信する手段とを備え、

前記第一の暗号化鍵の暗号化手段は、信号送受信時に経由し、かつ開示のみも

しくは開示と変更の両方を許容された他のセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、該生成した第一の暗号化鍵を暗号化し、

前記送信手段は、該暗号化された生成した第一の暗号化鍵と、該生成した第一の暗号化鍵により暗号化された信号と、第二の暗号化鍵が該他のセッション制御サーバの暗号化鍵である場合には、該他のセッション制御サーバに対する復号化要求指示、もしくは復号化要求指示と変更許容通知を送信することを特徴とするセッション制御サーバ。

【請求項４】　請求項２または請求項３記載のセッション制御サーバにおいて、

前記第一の暗号化鍵を、セッションと対向装置単位に保管もしくは記憶する手段と、

該第一の暗号化鍵を、同一セッションで、かつ同一対向装置内の信号の暗号化、復号化に再利用する再利用手段とを備えたことを特徴とするセッション制御サーバ。

【請求項５】　ネットワークを介してセッション制御サーバと通信可能に接続され、前記セッション制御サーバとの間で信号送受信により他の通信装置とのセッションを確立する着信側通信装置において、

暗号化した第一の暗号化鍵を添付して、暗号化された信号を受信する手段と、

該第一の暗号化鍵を復号化する手段と、

信号を該第一の暗号化鍵で復号化する手段と、

セッションと対向装置単位に該第一の暗号化鍵を保管あるいは記憶する手段と、

該第一の暗号化鍵を用いて信号を暗号化する手段と、

該第一の暗号化鍵で暗号化された信号を送信する手段とを備え、

該保管あるいは記憶する手段に保管あるいは記憶された第一の暗号化鍵を、同一セッション内の信号の暗号化、復号化に利用することを特徴とする着信側通信装置。

【請求項６】　請求項１記載の通信装置において、

前記第一の暗号化鍵を、セッションと対向装置単位に保管あるいは記憶する手段と、

該第一の暗号化鍵を用いて信号を暗号化する手段と、

該第一の暗号化鍵で暗号化された信号を送信する手段と、

該第一の暗号化鍵で暗号化された信号を受信する手段と、

該第一の暗号化鍵を用いて信号を復号化する手段とを備え、

該保管あるいは記憶する手段に保管あるいは記憶された第一の暗号化鍵を、同一セッション内の信号の暗号化、復号化に利用することを特徴とする発信側通信装置。

【請求項７】　請求項１，請求項５または請求項６のいずれかに記載の発信側または着信側の通信装置において、

前記セッションと対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段を備え、

該更新手段は、

新規に第一の暗号化鍵を生成する手段と、

該第一の暗号化鍵を、請求項１に記載の任意の第二の暗号化鍵、もしくは請求項５または６に記載の既に記憶された第一の暗号化鍵により暗号化する暗号化鍵暗号化手段と、

任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された信号を送信する手段とからなることを特徴とする通信装置。

【請求項８】　請求項１から請求項６までのいずれかに記載のセッション制御サーバにおいて、

前記セッションと対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段と、

請求項１または２に記載の任意の第二の暗号化鍵、もしくは請求項４，５または６に記載の既に記憶された第一の暗号化鍵により暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された信号を受信する手段と、

更新した新たに第一の暗号化鍵を用いて、信号を暗号化する手段と、

信号とともに更新された新たな暗号化鍵を送信する手段とを備え、

該送信手段は、請求項２に記載の任意の第二の暗号化鍵、もしくは請求項４に記載の既に記憶された第一の暗号化鍵で暗号化された、新たな第一の暗号化携を添付し、該第一の暗号化鍵で暗号化された信号を送信することを特徴とするセッション制御サーバ。

【請求項９】　ネットワークを介して互いに通信可能に接続され、通信装置相互間で信号送受信によりセッションを確立する通信システムにおいて、

暗号化した第一の暗号化鍵を添付して、該第一の暗号化鍵で暗号化された信号を受信する手段、自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗号化鍵を復号化する手段、復号化して得た第一の暗号化鍵を用いて信号を復号化する手段、復号化して得た第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段、任意の第二の暗号化鍵で暗号化した後、復号化して得た第一の暗号化鍵を添付して、復号化して得た第一の暗号化鍵で暗号化されている信号を送信する手段を備え、前記受信手段が暗号化された信号を受信した際に、復号化要求の有無を判断し、該第二の暗号化鍵に対応した第二の復号化鍵で暗号化鍵を復号化するか、あるいは、該第二の暗号化鍵に対応した第二の復号化鍵で該暗号化鍵を復号化することで、復号化要求の有無を判断するか、あるいは、その両方を行うことにより、該第一の暗号化鍵を取得し、前記信号復号化手段が該第一の暗号化鍵で暗号化された信号を復号化し、さらに、前記暗号化手段は、信号送受信時に経由し、かつ開示のみあるいは開示と変更の両方を許容された前記他のセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、取得された第一の暗号化鍵を暗号化し、前記送信手段は、該暗号化された第一の暗号化鍵と、取得された第一の暗号化鍵により暗号化されている信号と、第二の暗号化鍵が該他のセッション制御サーバの暗号化鍵である場合には、該他のセッション制御サーバに対する復号化要求指示を送信するセッション制御サーバと、

送信信号の守秘性を保つために暗号化した信号を送信する際に、暗号化のための第一の暗号化鍵を生成する手段、該第一の暗号化鍵を用いて信号を暗号化する手段、該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段、暗号化され

た該第一の暗号化鍵を添付して、該第一の暗号化鍵で暗号化された信号を送信する手段を備え、該第一の暗号化鍵を第二の暗号化鍵で暗号化する手段は、開示のみもしくは開示と変更の両方を許容された１つのセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、第一の暗号化鍵を暗号化し、該第一の暗号化鍵で暗号化された信号を送信する手段は、前記暗号化された第一の暗号化鍵と、該第一の暗号化鍵により暗号化された信号と、該第二の暗号化鍵が前記セッション制御サーバの暗号化鍵である場合には、該セッション制御サーバに対する復号化要求指示を送信する通信装置、あるいは、

前記各手段に加えて、送信信号の守秘性を保持するために暗号化した信号を送信する際に、暗号化のための新たな第一の暗号化鍵を生成する手段、生成した該第一の暗号化鍵を用いて信号を暗号化する手段、生成した該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する手段、該第二の暗号化鍵で暗号化した生成した第一の暗号化鍵を添付し、かつ該生成した第一の暗号化鍵で暗号化された信号を送信する手段を備え、前記第一の暗号化鍵の暗号化手段は、信号送受信時に経由し、かつ開示のみもしくは開示と変更の両方を許容された他のセッション制御サーバの第二の暗号化鍵、もしくは送信先の通信装置の第二の暗号化鍵により、該生成した第一の暗号化鍵を暗号化し、前記送信手段は、該暗号化された生成した第一の暗号化鍵と、該生成した第一の暗号化鍵により暗号化された信号と、第二の暗号化鍵が該他のセッション制御サーバの暗号化鍵である場合には、該他のセッション制御サーバに対する復号化要求指示を送信する通信装置と、

暗号化した第一の暗号化鍵を添付して、暗号化された信号を受信する手段と、

該第一の暗号化鍵を復号化する手段、信号を該第一の暗号化鍵で復号化する手段、セッションと対向装置単位に該第一の暗号化鍵を保管あるいは記憶する手段、該第一の暗号化鍵を用いて信号を暗号化する手段、該第一の暗号化鍵で暗号化された信号を送信する手段を備え、該保管あるいは記憶する手段に保管あるいは記憶された第一の暗号化鍵を、同一セッション内の信号の暗号化、復号化に利用する着信側通信装置と、

前記第一の暗号化鍵を、セッションと対向装置単位に保管あるいは記憶する手段、該第一の暗号化鍵を用いて信号を暗号化する手段、該第一の暗号化鍵で暗号

化された信号を送信する手段、該第一の暗号化鍵で暗号化された信号を受信する手段、該第一の暗号化鍵を用いて信号を復号化する手段を備え、該保管あるいは記憶する手段に保管あるいは記憶された第一の暗号化鍵を、同一セッション内の信号の暗号化、復号化に利用する発信側通信装置とを有することを特徴とする通信システム。

【請求項１０】　請求項９記載の通信システムにおいて、

前記第一の暗号化鍵を、セッションと対向装置単位に保管もしくは記憶する手段、該第一の暗号化鍵を、同一セッションで、かつ同一対向装置内の信号の暗号化、復号化に再利用する再利用手段を備えたセッション制御サーバと、

暗号化した第一の暗号化鍵を添付して、暗号化された信号を受信する手段、第一の暗号化鍵を復号化する手段、信号を該第一の暗号化鍵で復号化する手段、セッションと対向装置単位に該第一の暗号化鍵を保管あるいは記憶する手段、該第一の暗号化鍵を用いて信号を暗号化する手段、該第一の暗号化鍵で暗号化された信号を送信する手段を備え、該保管あるいは記憶する手段に保管あるいは記憶された第一の暗号化鍵を、同一セッション内の信号の暗号化、復号化に利用する着信側通信装置と、

前記第一の暗号化鍵を、セッションと対向装置単位に保管あるいは記憶する手段、該第一の暗号化鍵を用いて信号を暗号化する手段、該第一の暗号化鍵で暗号化された信号を送信する手段、該第一の暗号化鍵で暗号化された信号を受信する手段、該第一の暗号化鍵を用いて信号を復号化する手段を備え、該保管あるいは記憶する手段に保管あるいは記憶された第一の暗号化鍵を、同一セッション内の信号の暗号化、復号化に利用する発信側通信装置と

を有することを特徴とする通信システム。

【請求項１１】　請求項９記載の通信システムにおいて、

前記セッションと対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段、請求項１または２に記載の任意の第二の暗号化鍵、もしくは請求項４，５または６に記載の既に記憶された第一の暗号化鍵により暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化携で暗号化された信号を受信する手段、更新した新たな第一の暗号化鍵を用いて、信号を暗号化する手段、信号とともに

更新された新たな暗号化鍵を送信する手段を備え、前記送信手段は、請求項２に記載の任意の第二の暗号化鍵、もしくは請求項４に記載の既に記憶された第一の暗号化鍵により暗号化された、新たな第一の暗号化鍵を添付し、該第一の暗号化鍵で暗号化された信号を送信するセッション制御サーバと、

前記第一の暗号化鍵を、セッションと対向装置単位に保管あるいは記憶する手段、該第一の暗号化鍵を用いて信号を暗号化する手段、該第一の暗号化鍵で暗号化された信号を送信する手段、該第一の暗号化鍵で暗号化された信号を受信する手段、該第一の暗号化鍵を用いて信号を復号化する手段を備え、該保管あるいは記憶する手段に保管あるいは記憶された第一の暗号化鍵を、同一セッション内の信号の暗号化、復号化に利用する発信側通信装置と、

前記セッションと対向装置単位に管理した第一の暗号化鍵を周期的に更新する手段を備え、該更新手段は、新規に第一の暗号化鍵を生成する手段、該第一の暗号化鍵を、任意の第二の暗号化鍵により暗号化する暗号化鍵暗号化手段、任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された信号を送信する手段とからなる発信側または着信側通信装置とを有することを特徴とする通信システム。

【請求項１２】　発信側通信装置で生成したセッション制御信号を、信頼されるセッション制御サーバと、信頼されないセッション制御サーバとを経由して着信側通信装置に送信する通信方法において、

該発信側通信装置は、暗号化に使用した第一の暗号化鍵を、セッション制御サーバの公開された第二の暗号化鍵で暗号化し、

また、該セッション制御サーバに復号化要求を示す値と、復号化すべきコンテンツＩＤを含めて送信し、

該セッション制御サーバは、復号化要求パラメータの値で復号化要求を判断するか、暗号化された第一の暗号化鍵が設定されたデータの復号化可否で復号化要求を判断し、

復号化要求が有る場合には、第二の暗号化鍵に対応した第二の復号化鍵で復号化して、通信装置間制御情報の参照あるいは変更を可能とし、

通信装置間制御情報を変更した後、該第一の暗号化鍵をそのまま利用するか、

あるいは新規に生成した第一の暗号化鍵を用いて、変更後の情報を暗号化し、

次のセッション制御サーバあるいは着信側通信装置に送信することを特徴する通信方法。

【請求項１３】　セッション制御サーバが、セッション確立中に得られた情報を元に、ＮＡＴ／ファイヤウォール装置のフィルタリング条件を変更する通信方法において、

セッション制御サーバは、復号化する復号化鍵を判断した後、第一の暗号化鍵の復号化を行い、暗号化情報を該第一の暗号化鍵で復号化して通信装置間の制御情報を参照あるいは変更可能とし、

該制御情報を元に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求し、

その後、着信側通信装置から受信した通信装置間の制御情報を復号化して通信装置間の制御情報を参照あるいは変更可能とし、

該制御情報を元に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求し、ＮＡＴ／ファイヤウォール装置において通信装置相互間の主情報についてパケット通過を行わせることを特徴とする通信方法。

【請求項１４】　セッション制御サーバが、セッション確立中に得られた情報を元に、暗号化された主情報について通信記録を可能にする通信方法において、

セッション制御サーバは、ＮＡＴ／ファイヤウォール装置等に対してフィルタリング条件の変更要求に加え、主情報転送を指示し、ＮＡＴ／ファイヤウォール装置等から主情報を受信すると、該主情報が暗号化されている場合には、信号送受の際、請求項１３に記載の制御情報とともに、既に取得済みの主情報暗号化の鍵を用いて復号化し、該主情報を通信記録手段に記録することを特徴とする通信方法。

【請求項１５】　発信側通信装置で生成したセッション制御信号を、信頼されるセッション制御サーバと、信頼されないセッション制御サーバとを経由して着信側通信装置に送信する通信用プログラムであって、

該セッション制御サーバのコンピュータに、復号化要求パラメータの値で復号

化要求を判断するか、暗号化された第一の暗号化鍵が設定されたデータの復号化可否で復号化要求を判断する手順、復号化要求が有る場合には、第二の暗号化鍵に対応した第二の復号化鍵で復号化して、通信装置間制御情報の参照あるいは変更を可能とする手順、該第一の暗号化鍵をそのまま利用するか、あるいは新規に生成した第一の暗号化鍵を用いて、変更後の情報を暗号化する手順、次のセッション制御サーバあるいは着信側通信装置に送信する手順を、それぞれ実行させるための通信用プログラム。

【請求項１６】　セッション制御サーバが、セッション確立中に得られた情報を元に、ＮＡＴ／ファイヤウォール装置のフィルタリング条件を変更する通信用プログラムであって、

該セッション制御サーバのコンピュータに、復号化する復号化鍵を判断する手順、第一の暗号化鍵の復号化を行う手順、暗号化情報を該第一の暗号化鍵で復号化して通信装置間の制御情報を参照あるいは変更可能にする手順、該制御情報を元に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求する手順、着信側通信装置から受信した通信装置間の制御情報を復号化して通信装置間の制御情報を参照あるいは変更可能とする手順、該制御情報を元に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求する手順を、それぞれ実行させるための通信用プログラム。

【請求項１７】　セッション制御サーバが、セッション確立中に得られた情報を元に、暗号化された主情報について通信記録を行う通信用プログラムであって、

該セッション制御サーバのコンピュータに、ＮＡＴ／ファイヤウォール装置等に対してフィルタリング条件の変更要求に加え、主情報転送を指示する手順、ＮＡＴ／ファイヤウォール装置等から主情報を受信する手順、該主情報が暗号化されている場合には、信号送受の際、請求項１３に記載の制御情報とともに、既に取得済みの主情報暗号化の鍵を用いて復号化する手順、該主情報を通信記録手段に記録する手順を、それぞれ実行させるための通信用プログラム。

【請求項１８】　請求項１５から請求項１７までのいずれかに記載の通信用プログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、信号の中継を行うセッション制御サーバ、暗号鍵に基づいて暗号化された通信を行う通信装置と通信システムと通信方法、ならびにそれらを用いたプログラムとそれを記録した記録媒体に関する。

【０００２】

【従来の技術】

従来より、ユーザ間の通信情報の暗号化方式としては、ＩＰＳｅｃ（Ｓｅｃｕｒｉｔｙ ａｒｃｈｉｔｅｃｔｕｒｅ ｆｏｒ Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）、ＴＬＳ（Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ）、Ｓ／ＭＩＭＥなどが挙げられる。

中継サーバが、情報を参照できる暗号化方式としては、ＩＰＳｅｃ、ＴＬＳがある。

ＩＰＳｅｃは、ＴＰＣ／ＩＰの通信のセキュリティを強化するための技術であって、データをＩＰカプセル化してトンネリングする手法を規定するＥＳＰ（Ｅｎｃａｐｓｕｌａｔｉｏｎ Ｓｅｃｕｒｅ Ｐａｙｌｏａｄ）、ユーザ認証用のデータをＩＰデータに組み込むＡＨ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｈｅａｄｅｒ）などがある。ＴＬＳは、バンキングシステムなどエンド・エンドのセキュリティが必要なアプリケーションで広く用いられる。

【０００３】

ＩＰＳｅｃやＴＬＳの方法では、転送区間の始点、終点間で、暗号化鍵や方式の調整を行い、その結果に基づく暗号化通信を行い、通信装置が送受する伝達情報の機密性を向上させている。

上記に関しては、インターネットの標準化機関であるＩＥＴＦ（Ｉｎｔｅｒｎｅｔ Ｅｎｇｉｎｅｅｒｉｎｇ Ｔａｓｋ Ｆｏｒｃｅ）がとりまとめている規格書の中で、ＲＦＣ（Ｆｒｅｑｕｅｓｔ ｆｏｒ Ｃｏｍｍｅｎｔｓ）３２６１ Ｓｅｃｔｉｏｎ２６．２（非特許文献１参照）がある。

【０００４】

【非特許文献１】

ＲＦＣ３２６１Ｓｅｃｔｉｏｎ２６．２

【０００５】

【発明が解決しようとする課題】

ＩＰＳｅｃやＴＬＳなどの暗号化方式では、転送区間の始点、終点間で暗号化方式、鍵の調整を行い、暗号化／復号化の処理を転送区間の始点、終点で行う必要があった。そのため、信号中継を行うセッション制御サーバで、必ず信号の復号化を行うことになり、セッション制御サーバに対する情報保護が可能な暗号化通信が困難であった。

また、Ｓ／ＭＩＭＥの暗号化方式では、発着通信装置間で暗号化を行い、全てのセッション制御サーバに対して情報保護が可能であるが、特定のセッション制御サーバに情報開示が必要な場合であっても、情報開示が不可能であるという問題があった。

【０００６】

（目的）

本発明の目的は、上記のような従来の課題を解決するため、信頼できる宛先との間のセキュリティ確保が可能となるようなセッション制御サーバ、通信装置、通信システムおよび通信方法、ならびにそのプログラムと記録媒体を提供することにある。

上記セキュリティ確保の区間としては、転送区間に依存しない発ユーザと特定の信頼できるセッション制御サーバの間、特定の信頼できるセッション制御サーバと特定の信頼できるセッション制御サーバの間、および特定の信頼できるセッション制御サーバと着ユーザ間の任意の区間である。

【０００７】

【課題を解決するための手段】

本発明においては、信号の暗号化のために、通信装置もしくはセッション制御サーバで生成される暗号化鍵を第一の暗号化鍵と呼び、第一の暗号化鍵を暗号化するための暗号化鍵を第二の暗号化鍵と呼ぶ。

（１）通信装置Ａがセッション確立のための信号送信に先立ち、信号の暗号化の

ための第一の暗号化鍵（対称暗号鍵）を生成する。

送信先の通信装置Ｂの第二の暗号化鍵（公開鍵あるいは事前共有鍵）、もしくは、通信装置Ａがセッション確立に伴って情報の開示のみ、もしくは開示と変更の両方を許容するセッション制御サーバの第二の暗号化鍵（公開鍵あるいは事前共有鍵）のいずれかを用いて、第一の暗号化鍵を暗号化する。

通信装置Ａは、第一の暗号化鍵で暗号化した信号とともに、上記いずれかの第二の暗号化鍵（公開鍵あるいは事前共有鍵）で暗号化した第一の暗号化鍵と、第二の暗号化鍵がセッション制御サーバの暗号化鍵の場合は、さらに復号化要求指示をセッション制御サーバに送信する。

なお、ここでの復号化要求指示は、通信装置Ａがセッション確立に伴い情報の開示もしくは開示と変更を許諾する対象であるセッション制御サーバを、セッション制御サーバを示す識別子の形で陽に提示していてもよいし、陽に提示していなくてもよい。

【０００８】

陽に提示していない場合においては、例えば、セッション確立に伴い経由される個々のセッション制御サーバにおいて、自らの保持する第二の暗号化鍵に対応する第二の復号化鍵による第一の暗号化鍵の復号化を行い、得られた情報が第一の暗号化鍵を示す表現形式に合致しているとき、自らを復号化要求を受けたセッション制御サーバと判断できるため、第二の暗号化鍵で暗号化された第一の暗号化鍵自身が復号化要求指示となる。

また、ここでの情報の開示のみなのか、もしくは開示と変更の両方が許容されているか否かの違いは、例えば、対象となる情報に発信側通信端末による電子署名が付与されているか否か（例えば、付与されている場合は、開示のみが許容）などに依存させることもできる（請求項１参照）。

【０００９】

（２）通信装置Ａもしくは他のセッション制御サーバからの信号を受信したセッション制御サーバは、復号化要求有無を判断し、復号化要求があった場合、自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗号化鍵の復号化を行う。もしくは、自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗

号化鍵の復号化を行い、その結果から復号化要求有無を判断する。または、これらのいずれをも行う。これらは、（１）および（２）の後半に記載の通信装置およびセッション制御サーバにおける復号化要求に依存する。

いずれの場合においても、得られた第一の暗号化鍵を用いて、暗号化信号の復号化を行う。

次に、復号化して得た第一の暗号化鍵を、次段のセッション制御サーバあるいは着ユーザの第二の暗号化鍵（公開鍵あるいは事前共有鍵）で暗号化する。そして、第一の暗号化鍵で暗号化された信号、および第二の暗号化鍵で暗号化された第一の暗号化鍵を、セッション制御サーバあるいは着ユーザに送信する。なお、送信の際に、第二の暗号化鍵がセッション制御サーバの暗号化鍵の場合には、さらに復号化要求指示もセッション制御サーバに送信する（請求項２参照）。

【００１０】

（３）なお、上記（２）のセッション制御サーバにおいて、新たに第一の暗号化鍵（対称暗号鍵）を生成し、その鍵で復号化された信号の暗号化を行ってもよい。そして、その生成された第一の暗号化鍵を、次段のセッション制御サーバあるいは着ユーザの第二の暗号化鍵（公開鍵あるいは事前共有鍵）で暗号化する。それらを、セッション制御サーバあるいは着ユーザに送信する。なお、送信の際に、第二の暗号化鍵がセッション制御サーバの暗号化鍵の場合には、さらに復号化要求指示もセッション制御サーバに送信する（請求項３参照）。

【００１１】

（４）セッション制御サーバは、受信した第一の暗号化鍵、生成した第一の暗号化鍵を、セッションと対向装置単位に管理する。その後の信号の暗号化、復号化に再利用する（請求項４参照）。

（５）通信装置Ｂは、暗号化した第一の暗号化鍵を添付した暗号化信号を受信し、暗号化鍵の復号化を行い、その第一の暗号化鍵を用いて、暗号化信号の復号化を行う。応答信号を送信する際には、その復号化した第一の暗号化鍵を再利用して、信号を暗号化する。第一の暗号化鍵を添付せず、暗号化した信号を送信する。第一の暗号化鍵を記憶または保管し、同一セッションでかつ同一対向装置の信号の暗号化、および復号化に再利用する（請求項５参照）。

（６）通信装置Ａは、セッションと対向装置単位に第一の暗号化鍵を記憶または保管し、第一の暗号化鍵を暗号化した情報が添付されない暗号化情報を含む信号を受信した際に、同一セッションでかつ同一対向装置の信号の復号化に利用する。また、同一セッションでかつ同一対向装置の信号送信の際の情報の暗号化に、前記第一の暗号化鍵を再利用する（請求項６参照）。

【００１２】

（７）通信装置Ａ、および通信装置Ｂは、セッション内で一定時間経過あるいは一定回数使用後に、第一の暗号化鍵を更新し、更新信号と共に送信する（請求項７参照）。

（８）セッション制御サーバは、通信装置Ａ（あるいは通信装置Ｂ）より、更新信号を受信した際に、保管していた第一の暗号化鍵を更新し、更新信号を通信装置Ｂ（あるいは通信装置Ａ）に送信する。その際に、新たに生成した第一の暗号化鍵を生成して、通信装置Ｂ（あるいは通信装置Ａ）に送信してもよい（請求項８参照）。

本発明においては、情報開示を行うセッション制御サーバを指定して、情報開示を行える安全な信号の送受信が可能となる。特定のセッション制御サーバが信号情報の参照／変更が可能となるため、その信号情報をもとに通信制御が可能になる。

【００１３】

【発明の実施の形態】

以下、本発明の実施の形態を、図面により詳細に説明する。

（システム構成）

図１は、本発明の実施の形態に係る通信システムの構成図である。

図１に示すように、通信システム１００は、ネットワーク１０を介して通信可能に接続された複数のセッション制御サーバ１０１と、複数の通信装置１０２と、ＮＡＴ／ファイヤウォール装置１０３と、ネットワーク１０とを含むように構成される。

また、通信装置１０２は、本発明による手順に従ってセッション制御サーバ１０１を介して暗号化信号により通信を行う。なお、通信システム１００において

は、セッション制御サーバ１０１は２台示されているが、２台に限定されるものではない。また、通信装置１０２が２台示されているが、これも２台に限定されるものではない。また、ＮＡＴ／ファイヤウォール装置１０３が１台示されているが、これも１台に限定されるものではない。

【００１４】

なお、本発明においては、通信装置１０２は、パソコン、携帯端末、ゲートウェイなどの通信機器を含み、ネットワーク１０の構成は有線、無線を問わない。

これ以降は、説明の便宜を図るために、通信装置１０２－１を発信側とし、通信装置１０２－２を着信側として説明する。

通信装置１０２－１が、暗号化信号とともにセッション制御サーバ１０１－１用第二の暗号化鍵で暗号化した第一の暗号化鍵を、セッション制御サーバ１０１－１に送信する。セッション制御サーバ１０１－１が、通信装置１０２－１から送信された暗号化信号と暗号化した第一の暗号化鍵を受信して、セッション制御サーバ１０１－１用第二の暗号化鍵に対応する復号化鍵で、第一の暗号化鍵を復号化し、その第一の暗号化鍵で暗号化信号を復号化することにより、信号の参照／変更が可能となる。

【００１５】

セッション制御サーバ１０１－１は、受信した第一の暗号化信号（あるいは新規に作成した第一の暗号化信号）を使用して情報を暗号化し、暗号化に使用した第一の暗号化鍵を、通信装置１０２－２用の第二の暗号化鍵で暗号化し、セッション制御サーバ１０１－２に送信する。

セッション制御サーバ１０１－２は、セッション制御サーバ１０１－１から送信された暗号化信号と第一の暗号化鍵を受信する。しかし、これらを復号できないため、暗号化された情報は参照できない。セッション制御サーバ１０１－２は、受信した暗号化信号と暗号化した第一の暗号化鍵を、通信装置１０２－２に送信する。

通信装置１０２－２は、セッション制御サーバ１０１－２から受信した通信装置１０２－２用第二の暗号化鍵に対応する復号化鍵で、第一の暗号化鍵を復号化し、その第一の暗号化鍵で暗号化信号を復号化することにより、情報の参照が可

能となる。

通信装置１０２－２は、通信装置１０２－１に送信すべき応答信号などの信号を、復号化した暗号化鍵を再利用して暗号化し、セッション制御サーバ１０１－２、セッション制御サーバ１０１－１経由で通信装置１０２－１に送信する。

【００１６】

（通信装置）

図３は、本発明の実施形態に係る通信装置のブロック構成図である。

図３に示すように、通信装置１０２は、信号送信手段１２０、セッション制御手段１２１、暗号化鍵生成手段１２２、暗号化鍵暗号化手段１２３、信号暗号化手段１２４、暗号化鍵再利用手段１２５、信号復号化手段１２６、暗号化鍵復号化手段１２７、信号受信手段１２８、および暗号化鍵更新手段１２９を含むように構成される。

通信装置１０２－１は、セッション制御手段１２１で生成された信号のうち、機密性が必要な信号を暗号化鍵生成手段１２２で生成された暗号化鍵を使用して、信号暗号化手段１２４で暗号化する。

そして、その第一の暗号化鍵を開示先である特定のセッション制御サーバの公開鍵を使用して、暗号化鍵暗号化手段１２３により各々暗号化する。その際に、使用した暗号化鍵は、暗号化鍵再利用手段１２５にてセッションと対向装置に対応させて保管する。

【００１７】

セッション制御手段１２１で生成された信号のうち、暗号化していない信号に、セッション制御サーバに復号化を要求する情報を追加し、暗号化した信号と、暗号化した暗号化鍵とともに、信号送信手段１２０にてセッション制御サーバ１０１－１に送信する。これにより、機密性が必要な情報について、特定のセッション制御サーバ１０１－１に対してのみ開示可能な状態で、信号送信が可能となる。

【００１８】

図４は、本発明の実施形態に係る通信装置１０２－１の送信信号例の図である。

通信装置１０２－１からの送信信号は、ＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＩＮＶＩＴＥメソッドであって、そのメッセージに含まれる通信装置間の制御情報（ＳＤＰ：Ｓｅｓｓｉｏｎ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）４０５が暗号化されている。ＳＤＰには、通信装置１０２－１の主情報通信の情報として、受信用ＩＰアドレス、ポート番号などを含む。改竄防止のために、暗号化情報４０５には通信装置１０２－１のユーザのデジタル署名を添付してもよい。暗号化した情報は、Ｓ／ＭＩＭＥのＥｎｖｅｌｏｐｅｄ－Ｄａｔａ４０４として設定されている。その暗号化に使用した鍵（第一の暗号化鍵）は、セッション制御サーバの公開鍵（第二の暗号化鍵）で暗号化し、Ｅｎｖｅｌｏｐｅｄ－Ｄａｔａの中のＲｅｃｅｐｉｅｎｔＩｎｆｏ４０６として設定する。ＳＩＰメッセージ内の暗号化していない範囲４０１に、セッション制御サーバに復号化要求を示す値と、復号化すべきＣｏｎｔｅｎｔ－ＩＤを含んでいる。

改竄防止のために、ＳＩＰメッセージ４０２には、デジタル署名４０３を添付してもよい。

【００１９】

図５は、本発明の実施形態に係る通信装置１０２－２の送信信号例の図である。

通信装置１０２－２は、ＩＮＶＩＴＥメソッドに対する応答信号として２００ＯＫ５００を送信する。暗号化された情報５０５を送信する。改竄防止のために、ＳＩＰメッセージ５０２には、デジタル署名５０３を添付してもよい。

【００２０】

（セッション制御サーバ）

図２は、本発明の実施形態に係るセッション制御サーバのブロック構成図である。

図２に示すように、セッション制御サーバ１０１は、信号受信手段１１０、復号化判断手段１１１、暗号化鍵復号化手段１１２、復号化鍵再利用手段１１３、信号復号化手段１１４、セッション制御手段１１５、暗号化鍵生成手段１１６、暗号化鍵暗号化手段１１７、信号暗号化手段１１８、信号送信手段１１９を備える。それに加えて、ＮＡＴ／ファイヤウォール制御手段１３０、主情報通信受信

手段１３１、主情報復号化手段１３２を備えてもよい。

暗号化鍵復号化手段１１２は、信号復号化手段１１４の復号化鍵として第一の暗号化鍵を取得する手段を提供する。信号の復号化により、通信装置間の制御用の情報が参照可能となり、セッション制御手段１１５に必要な情報を提供する。

【００２１】

第一の暗号化鍵は、セッション制御手段１１５内のセッション識別子と対向装置識別子に対応して、復号化鍵再利用手段１１３において、復号化鍵を保管する。セッション制御手段１１５で、必要に応じて復号化した情報を参照／変更する。第一の暗号化鍵をそのまま利用して、あるいは、暗号化鍵生成手段１１６で第一の暗号化鍵を新規に生成し、暗号化鍵暗号化手段１１７で次段の信頼できるセッション制御サーバあるいは通信装置１０２－２の第二の暗号化鍵（公開鍵あるいは事前共有鍵）を暗号化する。そして、第一の暗号化鍵をそのまま利用するか、あるいは暗号化鍵生成手段１１６で生成した新規の第一の暗号化鍵を使用して、情報を暗号化する。

このように生成した暗号化情報、暗号化した暗号化鍵を、信号送信手段１１９により次段の信頼できるセッション制御サーバ、あるいは、通信装置１０２－２に送信する。

【００２２】

（第１の実施形態）

図６は、本発明の第１の実施形態に係る通信方法の説明図である。

ここでは、通信装置１０２－１で生成したセッション制御信号が、通信装置１０２－１から信頼されるセッション制御サーバ１０１－１へ、さらにセッション制御サーバ１０１－１からセッション制御サーバ１０１－２経由で通信装置１０２－２に送信される例を示している。

例えば、通信装置１０２－１からの送信信号は、ＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＩＮＶＩＴＥメソッドであり、そのメッセージに含まれる通信装置間の制御情報（ＳＤＰ）が暗号化されているものとする（図４の４０５参照）。ＳＤＰには、通信装置１０２－１の主情報通信の情報として、受信用ＩＰアドレス、ポート番号などを含んでいる。

ＳＩＰメッセージは、セッション制御サーバ１０１－１およびセッション制御サーバ１０１－２を経由して、通信装置１０２－２に送信される。

【００２３】

情報の暗号化に使用された鍵（第一の暗号化鍵）は、セッション制御サーバの公開鍵（第二の暗号化鍵）で暗号化され、Ｅｎｖｅｌｏｐｅｄ－Ｄａｔａの中のＲｅｃｅｐｉｅｎｔＩｎｆｏ（図４の４０６参照）として設定される。

また、第一の暗号化鍵は、セッション制御サーバ１０１－１と通信装置１０２－１の使用者間の事前共有鍵（パスワードなど）で暗号化されてもよい。

セッション制御サーバ１０１－１は、通信装置１０２－１から送信されたＩＮＶＩＴＥメソッドを信号受信手段１１０にて受信する。復号化判断手段１１１において、復号化要求パラメータ（例：Ｓｅｓｓｉｏｎ－Ｐｏｌｉｃｙ）の値で復号化要求を判断するか、あるいは、暗号化された第一暗号化鍵が設定されたＲｅｃｅｐｉｅｎｔＩｎｆｏ（図４の４０５参照）の復号化可否で復号化要求を判断してもよい。

【００２４】

復号化要求がある場合には、暗号化鍵復号化手段１１２は、第一の暗号化鍵の格納されたデータ（ＲｅｃｅｐｉｅｎｔＩｎｆｏ）（図４の４０６参照）の型を見て、どの第二の暗号化鍵に対応した第二の復号化鍵で復号化するかを判断した上で、第一の暗号化鍵の復号化を行い、信号復号化手段１１４に復号化鍵を渡す。暗号化情報の復号化により、通信装置間制御情報が参照／変更可能となり、セッション制御手段１１５に必要な情報を提供する。必要に応じて、セッション制御手段１１５にて通信装置間制御情報を変更する。次に、第一の暗号化鍵をそのまま利用するか、あるいは、暗号化鍵生成手段１１６にて新規に生成した第一の暗号化鍵を使用して、セッション制御手段１１５にて変更した後の情報を暗号化する。

【００２５】

第一の暗号化鍵は、通信装置１０２－１用の第二の暗号化鍵（公開鍵あるいは事前共有鍵）で暗号化する。セッション制御サーバ１０１－２が、信頼できる場合には、セッション制御サーバ１０１－２用の第二の暗号化鍵で暗号化してもよ

い。セッション制御サーバ１０１－１は、セッション制御手段１１５において、通信装置１０２－１から受信したＩＮＶＩＴＥメソッドについて処理（必要なパラメータ変更など）を行い、信号送信手段１１９よりセッション制御サーバ１０１－２に送信する。

セッション制御サーバ１０１－２は、セッション制御サーバ１０１－１から送信されたＩＮＶＩＴＥメソッドを信号受信手段１１０にて受信する。復号化判断手段１１１において、復号化要求パラメータ（例：Ｓｅｓｓｉｏｎ－Ｐｏｌｉｃｙ）の値で復号化要求を判断するか、あるいは、暗号化された第一の暗号化鍵が設定されたＲｅｃｅｐｉｅｎｔＩｎｆｏ（図４の４０６参照）の復号化可否で復号化要求を判断してもよい。

【００２６】

復号化要求がないか、あるいは、復号化不可のため、セッション制御手段１１５にて、参照可能な情報をもとにＩＮＶＩＴＥメソッドについて処理（必要なパラメータ変更など）を行い、信号送信手段１１９より通信装置１０２－２に送信する。

信号を受信した通信装置１０２－２は、信号受信手段１２８で受信した信号が暗号化されており、第一の暗号化鍵が暗号化されて添付されていると、自身の第二の暗号化鍵に対応する第二の復号化鍵（第一の暗号化鍵が公開の場合には秘密鍵、あるいは第一の暗号化鍵が事前共有鍵であれば同じ事前共有鍵）を使用して、暗号化鍵復号化手段１２７で復号化し、第一の暗号化鍵を得る。その第一の暗号化鍵を使用して、暗号化された情報を信号復号化手段１２６にて復号化することにより、情報が参照可能となる。その情報をセッション制御手段１２１に提示する。

【００２７】

セッション制御手段１２１は、必要に応じて送信すべき情報を生成するとともに、暗号化鍵を暗号化鍵再利用手段１２５にてセッションと対向装置対応に保管する。例えば、ＩＮＶＩＴＥメソッドに対する応答信号として、図５の５００を送信する。送信すべき情報について、保管もしくは記憶している第一の暗号化鍵を使用して、信号暗号化手段１２４により暗号化した情報を信号送信手段１２０

信号を送信する。

【００２８】

（応用例１：請求項６参照）

その後のセッションの継続信号が、例えばＭＥＳＳＡＧＥメソッドが通信装置１０２－１よりセッション制御サーバ１０１－１、１０１－２経由で通信装置１０２－２に送信される。通信装置１０２－１は、セッション単位に保管または記録している第一の暗号化鍵を使用してＭＥＳＳＡＧＥメソッドに設定する情報を暗号化する。第一の暗号化鍵を添付しないで、暗号化した情報を含むＭＥＳＳＡＧＥメソッドを送信する。

当該信号を受信した通信装置１０２－２は、暗号化鍵再利用手段１２５において、セッションと対向装置の識別子をキーに、保管している第一の暗号化鍵を取得し、その第一の暗号化鍵にて暗号化情報を復号化する。

【００２９】

（応用例２：請求項２，３参照）

セッション制御サーバ１０１－１においても、セッションと対向装置単位に保管している第一の暗号化鍵を使用して暗号化情報を復号化する。

（応用例３：請求項７参照）

また、一定時間経過後、通信装置１０２－１がＭＥＳＳＡＧＥメソッドをセッション制御サーバ１０１－１，１０１－２経由で通信装置１０２－２に送信する際に、暗号化鍵更新手段１２９にて第一の暗号化鍵を更新する。更新した暗号化鍵を用いて情報を暗号化し、Ｓ／ＭＩＭＥのＥｎｖｅｌｏｐｅｄ－Ｄａｔａとして設定する。

その暗号化に使用した鍵（更新した第一の暗号化鍵）は、セッション制御サーバの公開鍵（第二の暗号化鍵）で暗号化し、Ｅｎｖｅｌｏｐｅｄ－Ｄａｔａの中のＲｅｃｅｐｉｅｎｔＩｎｆｏとして設定する。

更新した第一の暗号化鍵を添付した暗号化信号を受信すると、通信装置１０２－２は、更新された第一の暗号化鍵を暗号化鍵再利用手段１２５にて保管あるいは記憶する。

【００３０】

（応用例４：請求項８参照）

更新した第一の暗号化鍵を添付した暗号化信号を受信したセッション制御サーバ１０１－１は、更新された第一の暗号化鍵を暗号化鍵再利用手段１２５にて保管あるいは記憶する。

【００３１】

（第２の実施形態）

図７は、本発明の第２の実施形態に係る通信方法の説明図である。

ここでは、セッション制御サーバ１０１－１が、セッション確立中に得られた情報を元にＮＡＴ／ファイヤウォール装置１０３のフィルタリング条件を変更する例を示している。

例えば、セッション制御サーバ１０１－１が通信装置１０２－１から受信した信号がＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＩＮＶＩＴＥメソッドであって、そのメッセージに含まれる通信装置間の制御情報（ＳＤＰ）が暗号化されているとする。セッション制御サーバ１０１－１では、暗号化鍵復号化手段１１２において、第一の暗号化鍵の格納されたデータ（ＲｅｃｅｐｉｅｎｔＩｎｆｏ）（図５の４０６参照）の型を見て、どの鍵で復号化するかを判断した上で、第一の暗号化鍵の復号化を行う。

【００３２】

暗号化情報（図５の４０５参照）を第一の暗号化鍵で復号化することで、通信装置間の制御情報（例えば、通信装置１０２－１の主情報通信径路のＩＰアドレスとポート番号）が参照／変更可能となる。

この情報を元に、ＮＡＴ／ファイヤウォール制御手段１３０において、遠隔のＮＡＴ／ファイヤウォール装置１０３に対してフィルタリング条件の変更（不特定ＩＰアドレスから特定ＩＰアドレス＋ポート番号宛のパケット通過指示）を要求する。

セッション制御サーバ１０１－１は、その後、通信装置１０２－２から受信した信号が、ＳＩＰメッセージの１つである２００　ＯＫ応答であって、そのメッセージに含まれる通信装置間の制御情報（ＳＤＰ）が暗号化されている。復号化鍵再利用手段１１３に記憶していた第一の暗号化鍵を用いて暗号化情報を復号化

することで、通信装置１０２－２の主情報通信径路のＩＰアドレスとポート番号が通信装置間の制御情報が参照可能となる。

【００３３】

この情報をもとに、ＮＡＴ／ファイヤウォール制御手段１３０において、遠隔のＮＡＴ／ファイヤウォール装置１０３に対して、フィルタリング条件の変更（特定ＩＰアドレスから特定ＩＰアドレス＋ポート番号宛のパケット通過指示）を要求する。これにより、ＮＡＴ／ファイヤウォール装置１０３において、通信装置１０２－１と通信装置１０２－２間の主情報についてパケット通過が可能となる。

その後、通信装置１０２－１あるいは１０２－２から受信したＳＩＰメッセージの切断信号であるＢＹＥメソッドを受信すると、セッション制御サーバ１０１－１は、ＮＡＴ／ファイヤウォール制御手段１３０において、ＮＡＴ／ファイヤウォール装置１０３に対してフィルタリング条件の変更（指定ＩＰアドレスから指定ＩＰアドレス＋ポート番号宛のパケット不通過指示）を要求する。

本実施形態で示したように、通信装置より信号内の情報を安全に開示されたセッション制御サーバ１０１－１により、セッション単位にＮＡＴ／ファイヤウォール制御を行え、アクセス制御の精度を高めることが可能になる。情報を開示されないセッション制御サーバ１０１－２は、主情報の径路情報が参照できないため、主情報のモニタが困難となり、主情報通信の機密性を高めることができる。

【００３４】

（第３の実施形態）

図８は、本発明の第３の実施形態に係る通信方法の説明図である。

ここでは、セッション制御サーバが、セッション確立中に得られた情報を元に、暗号化された主情報についても、通信記録が可能となる例を示している。

例えば、通信装置１０２－１からの送信信号は、ＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＩＮＶＩＴＥメソッドであって、そのメッセージに含まれる通信装置情報ＳＤＰが暗号化されている。ＳＤＰには、通信装置１０２－１、通信装置１０２－２間の主情報通信の際に使用するＩＰアドレス、ポート番号に加えて、主情報暗号化のための鍵情報を含む。

【００３５】

セッション制御サーバ１０１－１が、主情報通信記録の手段１３１と、主情報復号化手段１３２を備え、遠隔のＮＡＴ／ファイヤウォール装置１０３に対して指示を送信する。

第２の実施形態のフィルタリング条件変更要求に加えて、主情報転送を指示する。セッション制御サーバの主情報通信受信手段１３１にて、ＮＡＴ／ファイヤウォール装置１０３から主情報を受信する。主情報が暗号化されている場合には、既に取得済みの主情報暗号化の鍵情報を用いて、主情報復号化手段１３２にて復号化を行う。復号化が正常終了すると、その情報を記録する。

セッション制御サーバ１０１－２は、暗号化信号を復号化できないため、通信装置情報ＳＤＰは参照できず、ＳＤＰに含まれる主情報暗号化のための鍵情報は参照できない。そのため、ネットワーク内のモニタ装置で主情報をモニタしても、暗号化されており、それを復号化することができない。

【００３６】

このように、主情報が暗号化されている場合でも、特定の信頼できるセッション制御サーバによる復号化した主情報の記録が行え、通信情報の監査が可能となる。

このように、本実施形態に係る通信方法では、任意の信号中継を行うセッション制御サーバに対して、情報開示／変更を可能にして、情報を安全に送信し、特定のセッション制御サーバによる通信制御が可能になる。

【００３７】

なお、上記第１、第２および第３の実施形態で説明した手順をプログラム化し、そのプログラムをＣＤ－ＲＯＭなどの記録媒体に格納しておけば、プログラムの販売や貸与の場合に便利であり、また、セッション制御サーバのコンピュータや、通信装置のコンピュータに記録媒体を装着して、プログラムをインストールし、実行させることで、本発明を容易に実現することができる。

【００３８】

【発明の効果】

以上説明したように、本発明によれば、接続構成によらず、特定のセッション

制御サーバや着ユーザのみに、信号情報を開示させることが可能である。また、セッション制御サーバにより情報参照だけでなく、変更も可能である。

これにより、信頼できる宛先との間のセキュリティの確保が可能になるという顕著な効果を奏する。

【図面の簡単な説明】

【図１】

本発明の実施形態に係る通信システムの構成図である。

【図２】

図１におけるセッション制御サーバのブロック構成図である。

【図３】

図１における通信装置のブロック構成図である。

【図４】

本発明の実施形態に係る通信装置（１０２－１）の送信信号例の図である。

【図５】

本発明の実施形態に係る通信装置（１０２－２）の送信信号例の図である。

【図６】

本発明の第１の実施形態に係る通信方法の説明図である。

【図７】

本発明の第２の実施形態に係る通信方法の説明図である。

【図８】

本発明の第３の実施形態に係る通信方法の説明図である。

【符号の説明】

１０…ネットワーク、１０１－１，１０１－２…セッション制御サーバ、
１０２－１，１０２－２…通信装置、
１０３…ＮＡＴ／ファイヤウォール装置、１１０…信号受信手段、
１１１…復号化判断手段、１１２…暗号化鍵復号化手段、
１１３…復号化鍵再利用手段、１１４…信号復号化手段、
１１５…セッション制御手段、１１６…暗号化生成手段、
１１７…暗号化鍵暗号化手段、１１８…信号暗号化手段、

１１９…信号送信手段、１３０…ＮＡＴ／ファイヤウォール制御手段、

１３１…主情報通信受信手段、１３２…主情報復号化手段、

１２０…信号送信手段、１２１…セッション制御手段、

１２２…暗号化鍵生成手段、１２３…暗号化鍵暗号化手段、

１２４…信号暗号化手段、１２５…暗号化鍵再利用手段、

１２６…信号復号化手段、１２７…暗号化鍵復号化手段、

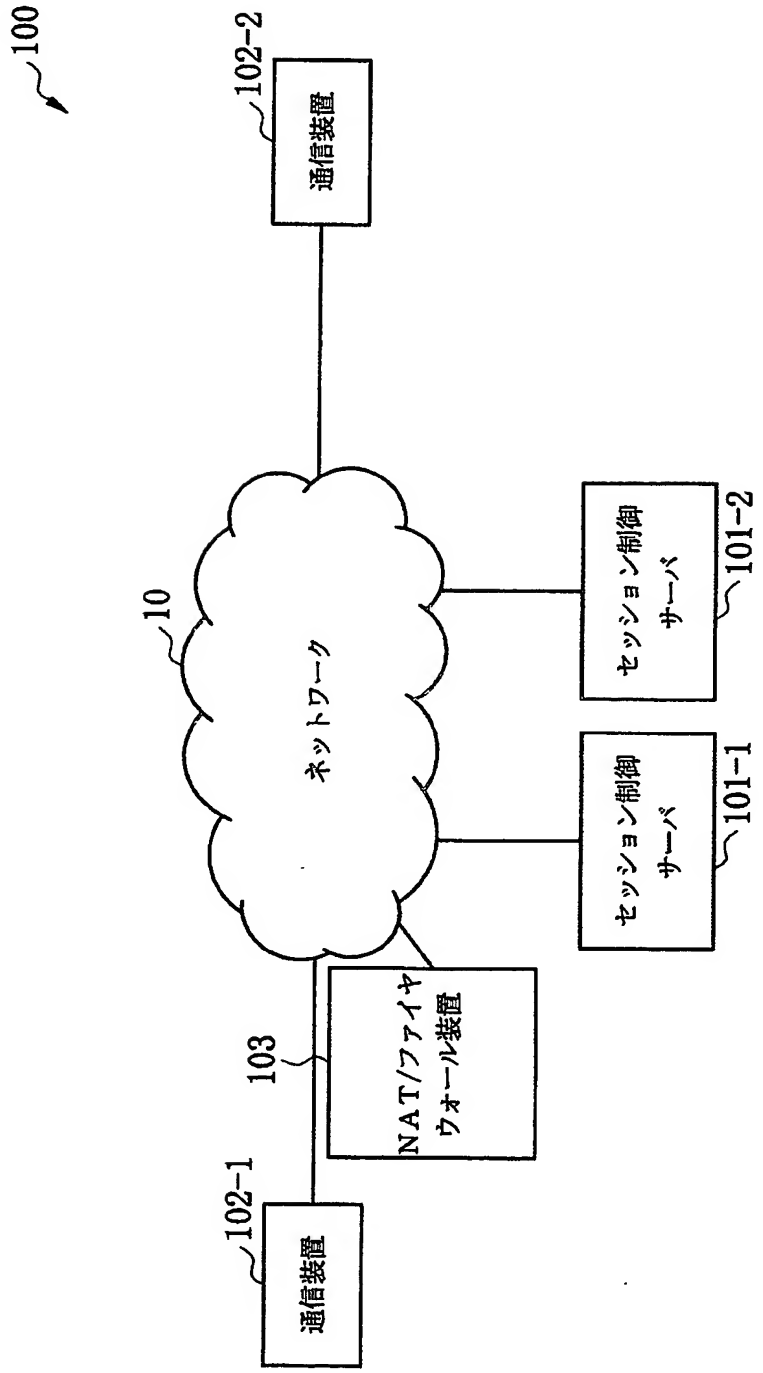
１２８…信号受信手段、１２９…暗号化更新手段、

４００～４０６…通信装置（１０２－１）の送信信号例の指定領域、

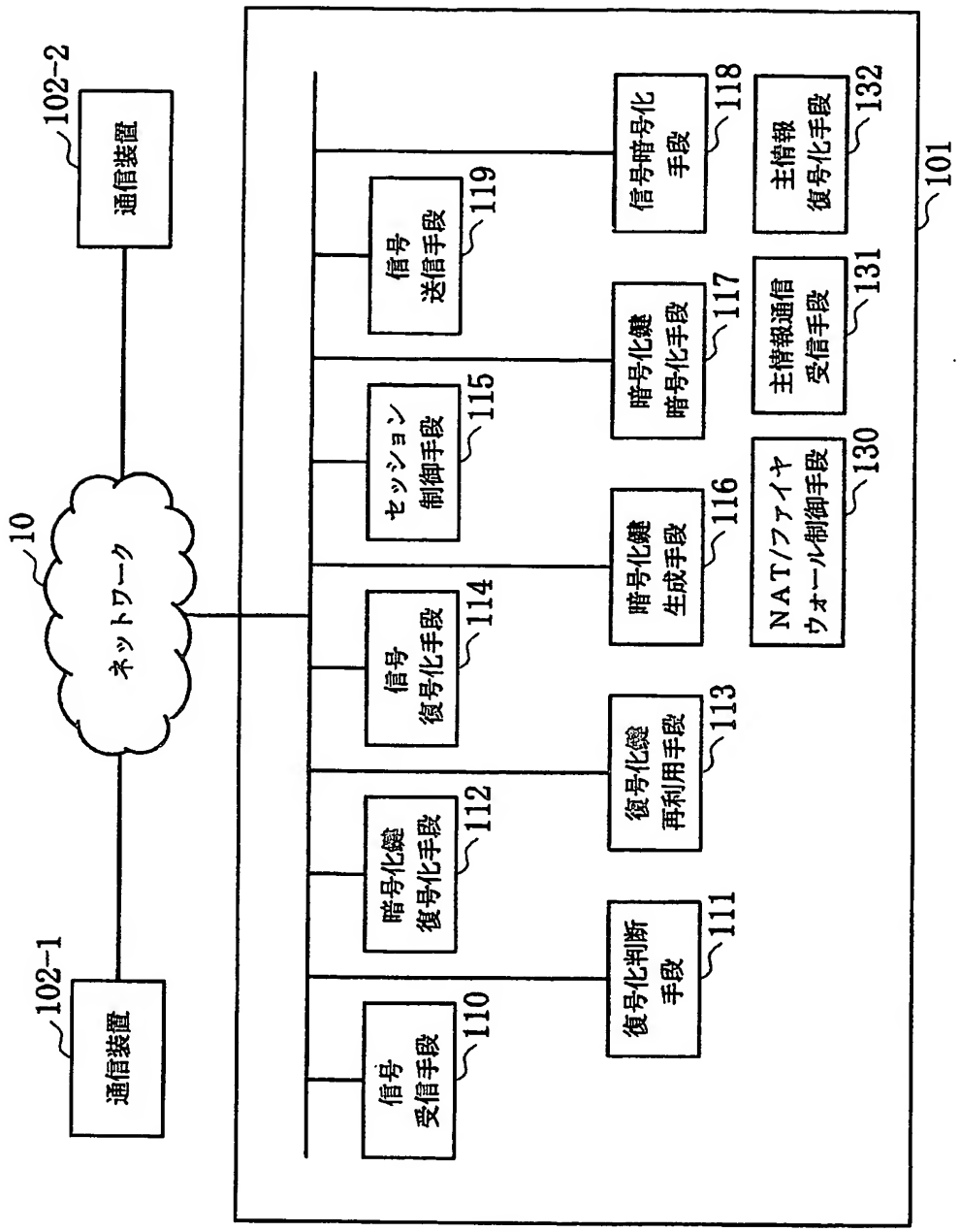
５００～５０５…通信装置（１０２－２）の送信信号例の指定領域。

【書類名】　図面

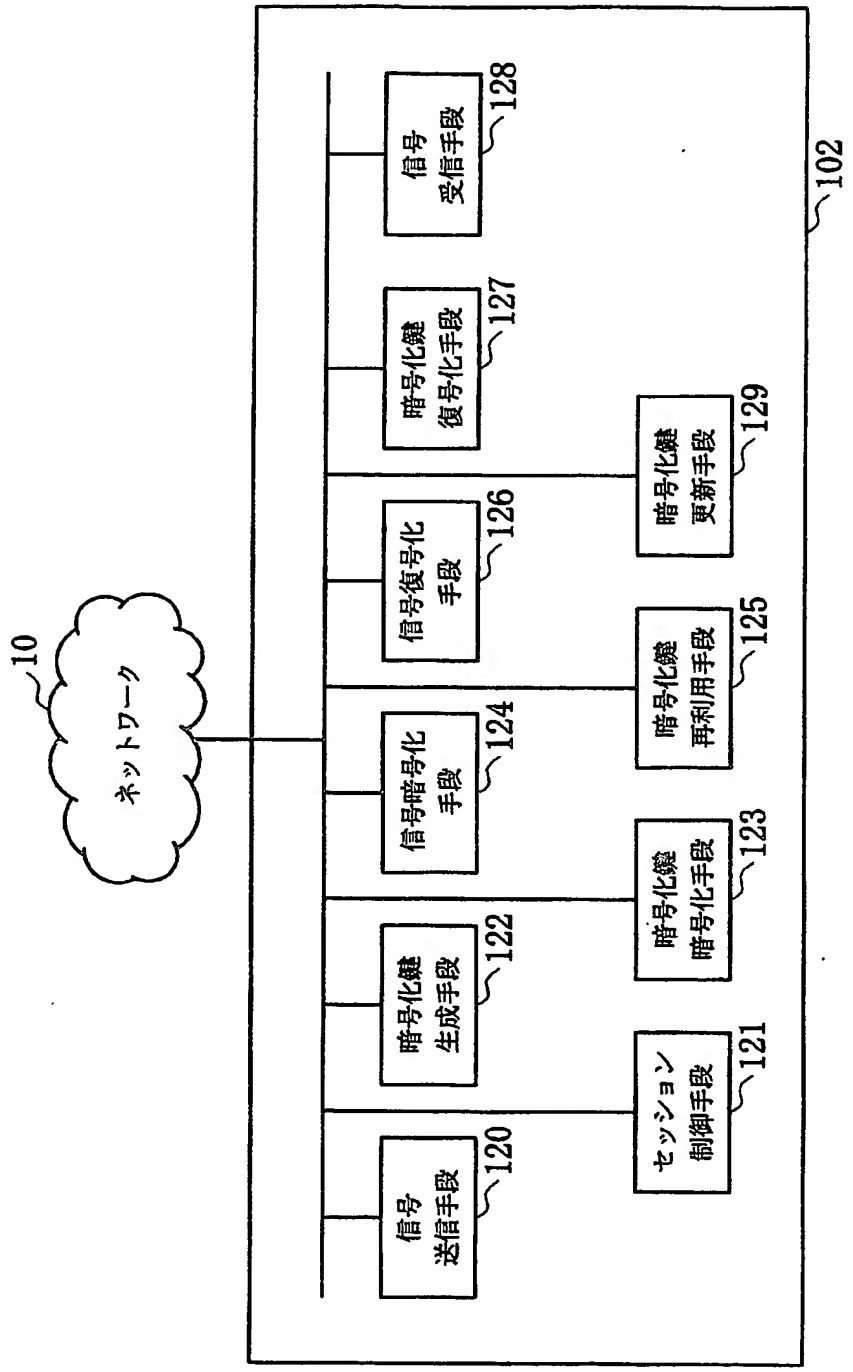
【図１】


100
102-2
通信装置
10
ネットワーク
セッション制御サーバ
101-2
セッション制御サーバ
101-1
103
NAT/ファイヤウォール装置
102-1
通信装置

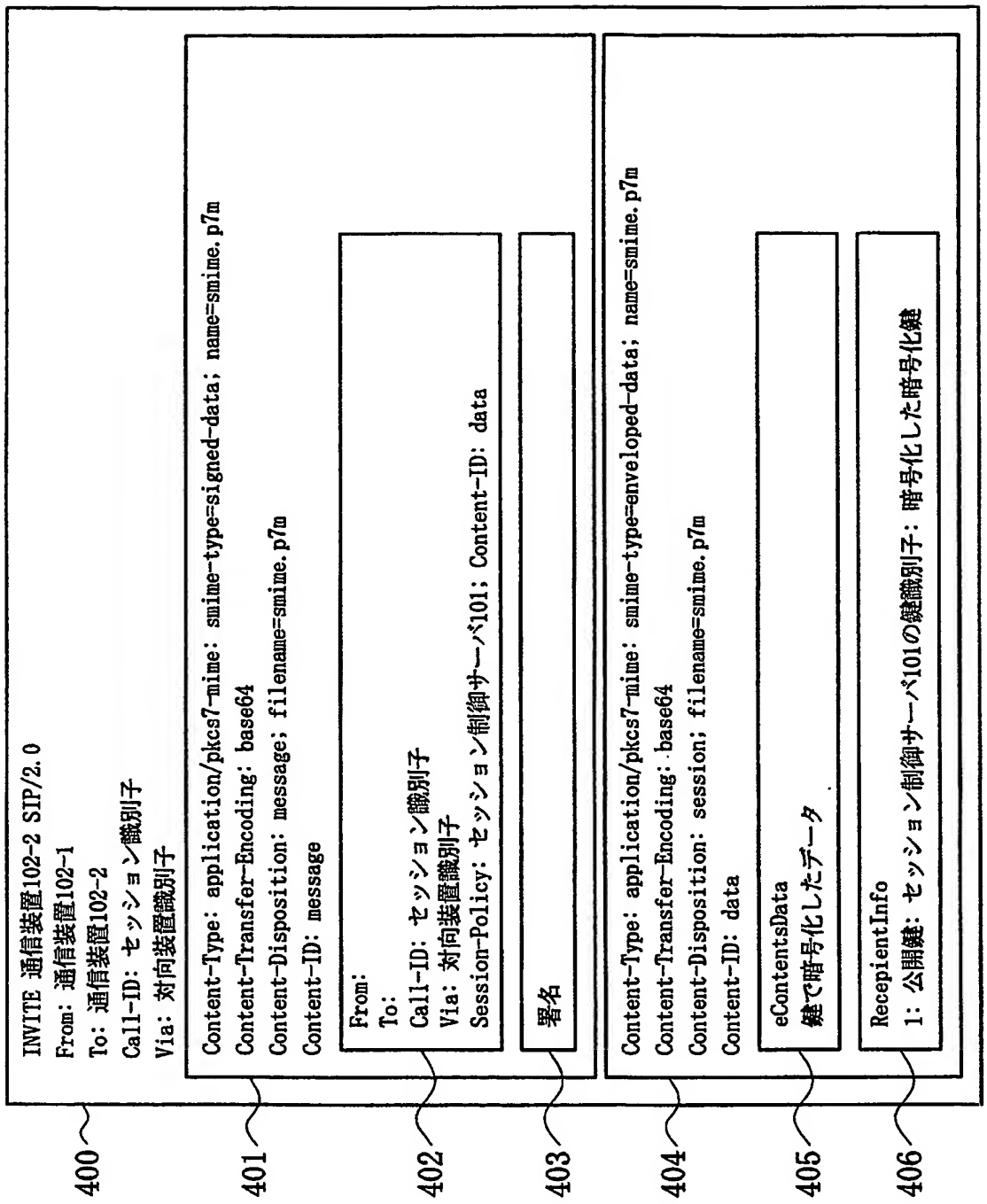
【図２】


102-2
通信装置
102-1
通信装置
10
ネットワーク
101
信号受信手段
110
暗号化鍵復号化手段
112
復号化判断手段
111
信号復号化手段
114
復号化鍵再利用手段
113
セッション制御手段
115
暗号化鍵生成手段
116
信号送信手段
119
暗号化鍵暗号化手段
117
信号暗号化手段
118
NAT/ファイヤウォール制御手段
130
主情報通信受信手段
131
主情報復号化手段
132

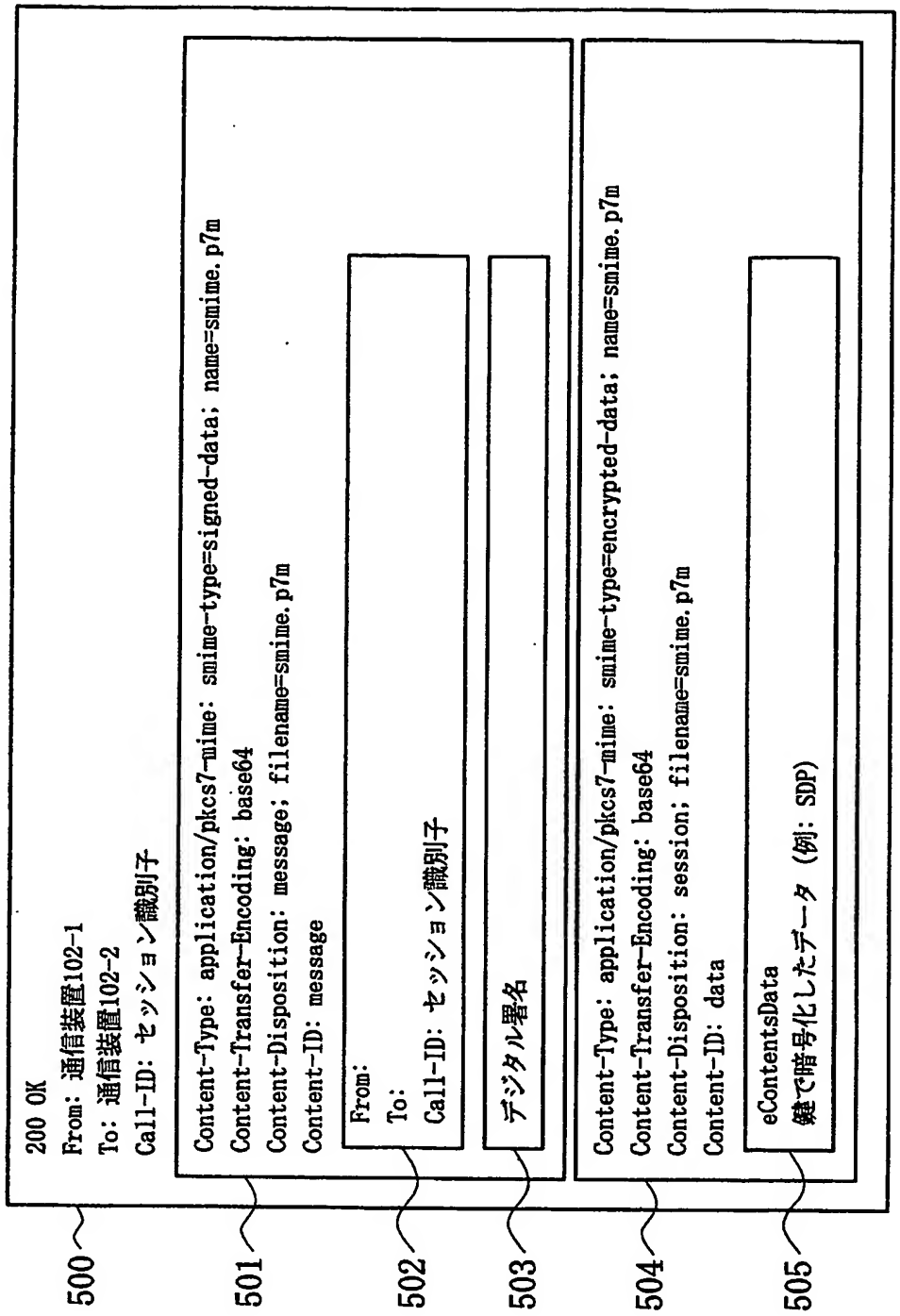
【図３】


10
ネットワーク
102
信号送信手段
120
暗号化鍵生成手段
122
信号暗号化手段
124
信号復号化手段
126
暗号化鍵復号化手段
127
信号受信手段
128
セッション制御手段
121
暗号化鍵暗号化手段
123
暗号化鍵再利用手段
125
暗号化鍵更新手段
129

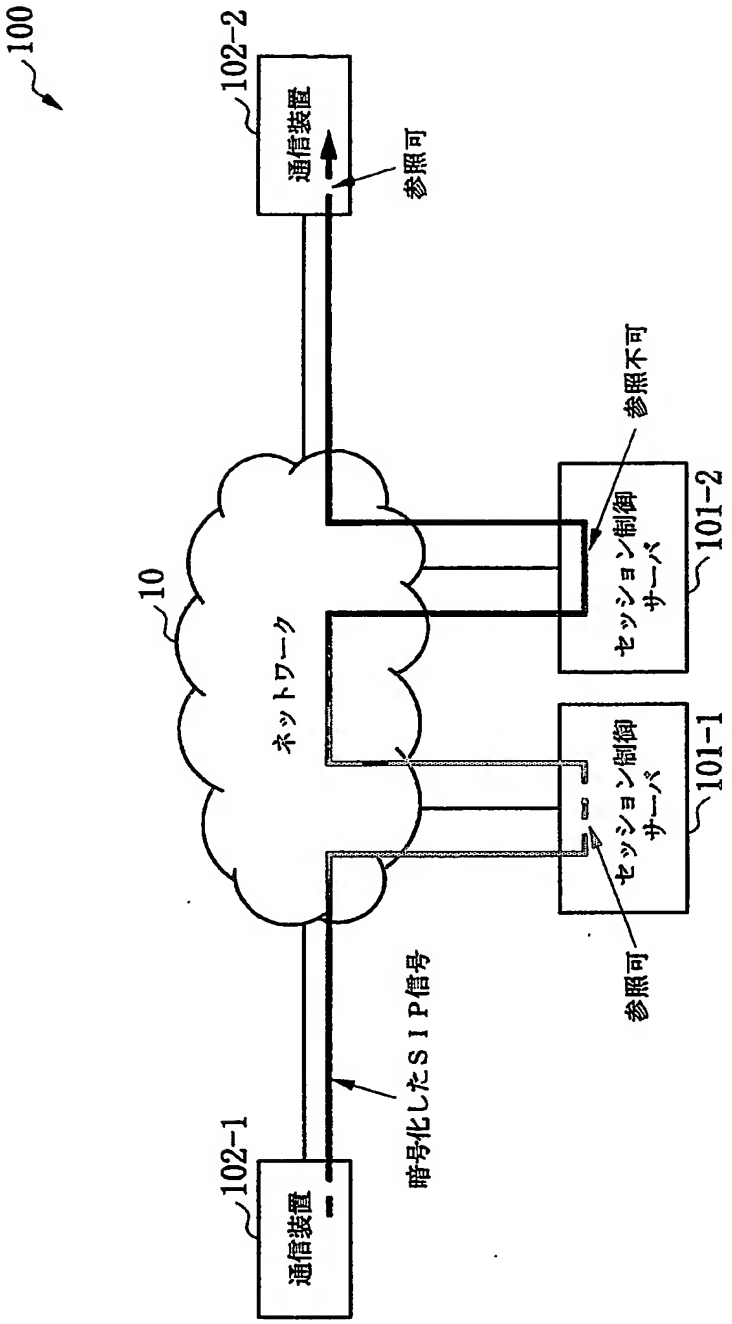
【図４】


400
INVITE 通信装置102-2 SIP/2.0
From: 通信装置102-1
To: 通信装置102-2
Call-ID: セッション識別子
Via: 対向装置識別子
401
Content-Type: application/pkcs7-mime; smime-type=signed-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: message; filename=smime.p7m
Content-ID: message
402
From:
To:
Call-ID: セッション識別子
Via: 対向装置識別子
Session-Policy: セッション制御サーバ101; Content-ID: data
403
署名
404
Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: session; filename=smime.p7m
Content-ID: data
405
eContentsData
鍵で暗号化したデータ
406
RecepientInfo
1: 公開鍵: セッション制御サーバ101の鍵識別子: 暗号化した暗号化鍵

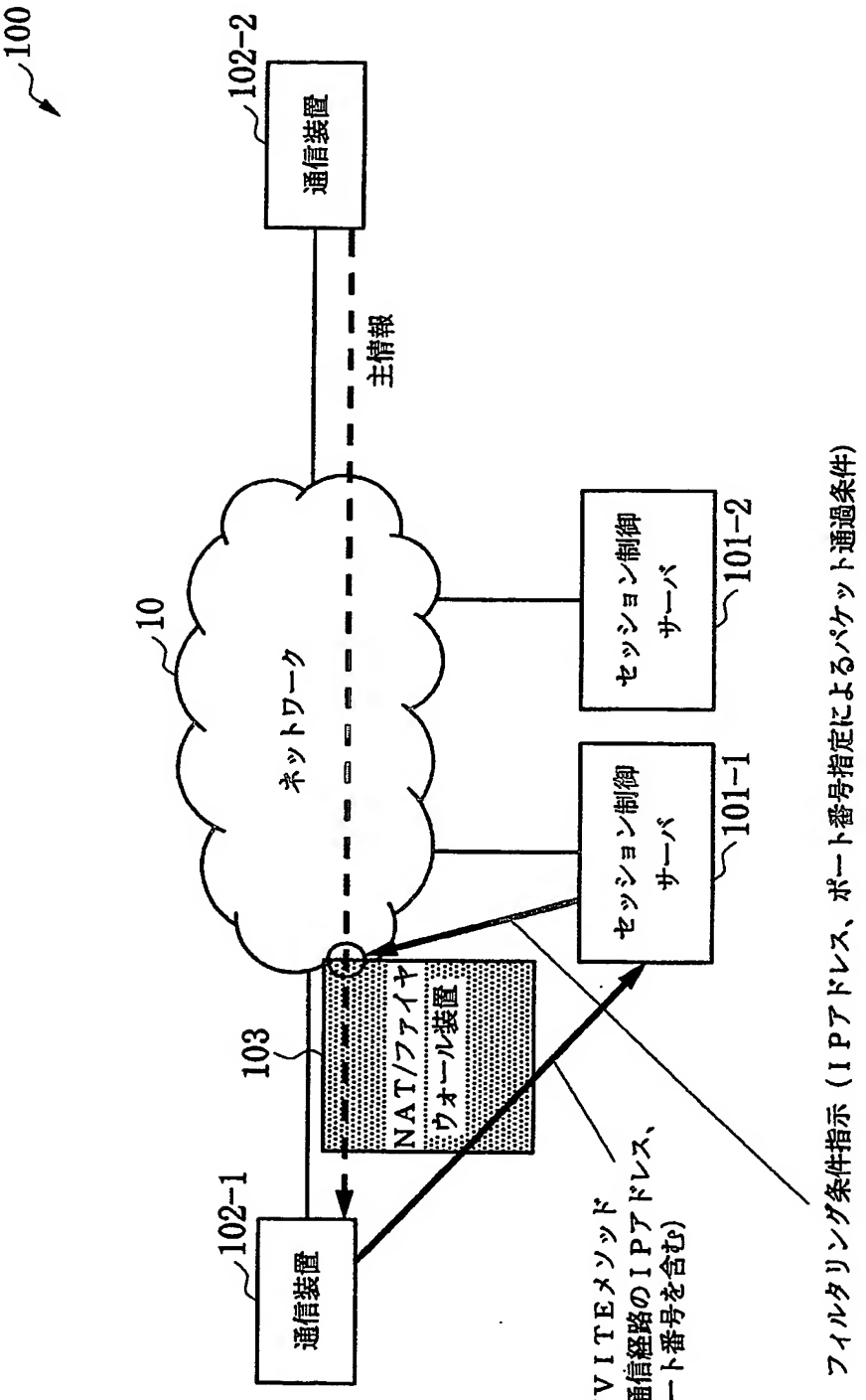
【図５】


200 OK
From: 通信装置102-1
To: 通信装置102-2
Call-ID: セッション識別子
500
Content-Type: application/pkcs7-mime; smime-type=signed-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: message; filename=smime.p7m
Content-ID: message
501
From:
To:
Call-ID: セッション識別子
502
デジタル署名
503
Content-Type: application/pkcs7-mime; smime-type=encrypted-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: session; filename=smime.p7m
Content-ID: data
504
eContentsData
鍵で暗号化したデータ（例：SDP）
505

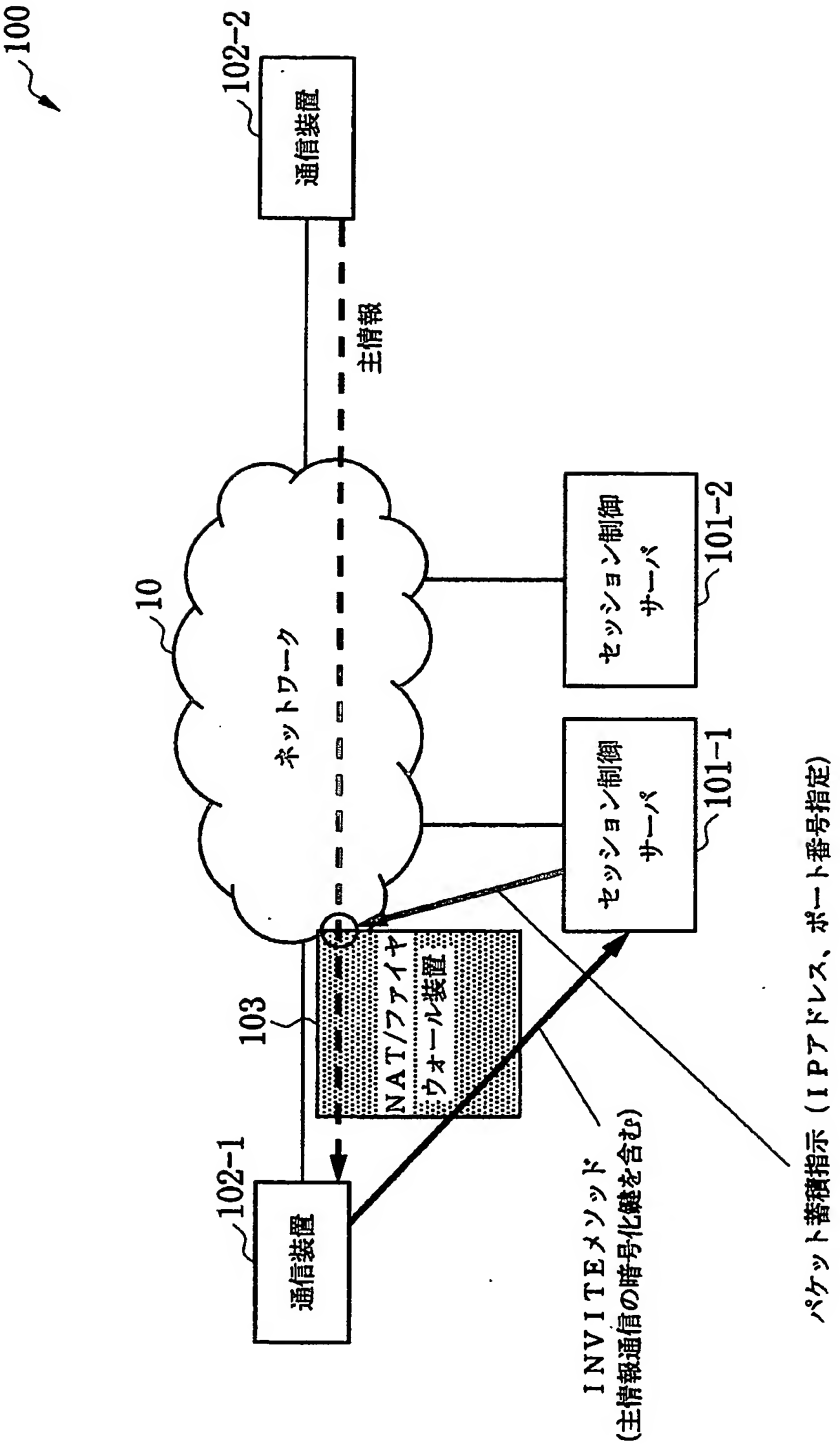
【図６】


100
102-2
通信装置
参照可
参照不可
10
ネットワーク
セッション制御サーバ
101-2
セッション制御サーバ
101-1
参照可
暗号化したＳＩＰ信号
102-1
通信装置

【図７】


100
102-2
通信装置
主情報
10
ネットワーク
セッション制御
サーバ
101-2
セッション制御
サーバ
101-1
103
NAT/ファイヤ
ウォール装置
102-1
通信装置
INVITEメソッド
(主情報通信経路のIPアドレス、
ポート番号を含む)
フィルタリング条件指示（IPアドレス、ポート番号指定によるパケット通過条件）

【図８】


100
102-2
通信装置
主情報
10
ネットワーク
セッション制御サーバ
101-2
セッション制御サーバ
101-1
103
NAT/ファイヤウォール装置
102-1
通信装置
INVITEメソッド
(主情報通信の暗号化鍵を含む)
パケット蓄積指示（IPアドレス、ポート番号指定）

【書類名】　　要約書

【要約】

【課題】接続構成によらず、特定の中継サーバに対して情報開示あるいは変更を可能にする。

【解決手段】通信装置１０２－１が送信情報を暗号化するのに使用する暗号化鍵を、情報開示したい特定の中継サーバ１０１－１あるいは１０１－２の公開鍵で暗号化し、それらの情報を暗号化鍵で暗号化した情報とともに送信する。その信号を受信した中継サーバ１０１－１は、必要に応じて参照または変更した後、暗号化鍵を次段の中継サーバ１０１－２あるいは着ユーザの通信装置１０２－２の公開鍵で暗号化し、それらの情報を暗号化鍵で暗号化した情報とともに送信する。また、暗号化鍵の暗号化に使用する鍵は、公開鍵の代わりに事前共有鍵も使用可能である。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２００３－１７６５６９
受付番号	５０３０１０３４２２０
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１５年　６月２３日

＜認定情報・付加情報＞

【提出日】　平成15年 6月20日

次頁無

出願人履歴情報

識別番号　[０００００４２２６]

１．変更年月日　１９９９年　７月１５日
[変更理由]　住所変更
住　所　東京都千代田区大手町二丁目３番１号
氏　名　日本電信電話株式会社